Defense Horizons
Number 50
A publication of the
Center for Technology and National Security Policy
National Defense University
OCTOBER 2005

Sweden's Use of Commercial Information Technology for Military Applications

by Franklin D. Kramer and John C. Cittadino

Overview

Sweden, a nation of only 9 million people with a political climate that has fostered a posture of nonalignment for over half a century, has nevertheless maintained highly credible, modern, and high-technology military forces. Sweden has expanded the mission of forces originally designed for the Cold War to include international peacekeeping. The focus of this study is the Swedish formula for achieving the high-technology military capabilities that successfully compensate for a small standing force. What policies and processes enabled the Swedish military to take advantage of leading-edge producers of commercial information technology (CIT)? What lessons does the Swedish model hold for the U.S. Department of Defense?

A National Defense University case study examined the Swedish experience, policy, process, and government-industry relationships to determine ways to improve America's ability to capitalize on the use of CIT in military systems. The case study included a review of published Swedish policies, regulations, and reports but is based predominantly on meetings and interviews with Swedish industry and government officials.

The case study found more similarities than differences in Swedish and American policies and processes for acquiring commercial technology for military systems. Perhaps the most significant difference is that in Sweden, government and industry participants in the acquisition process have embraced the policy for maximum utilization of CIT, whereas Americans still debate whether commercial technology can do the job in warfighter or other defense applications. Furthermore, Sweden has initiated an acquisition process that *routinely* examines all requirements to determine the potential to do the job with CIT and then performs tradeoff analyses to determine acceptance.

The Department of Defense (DOD) has entered the information age with a concept of network-centric warfare that relies on incorporation of state-of-the-art information technology (IT) in military systems. From major computer centers vital to managing the routine business of the department to frontline battlefield communications and automated, networked weapons systems, the demands for affordable, state-of-the-art IT products and services continue to increase. Much of the cutting edge of the IT sector is now found in the commercial world. Commercial research and development (R&D) investment is huge, and new products emerge every 12–18 months. To stay abreast of IT developments, DOD must take advantage of commercial information technology (CIT). Moreover, given other budget requirements, it makes little sense for DOD to fund the R&D necessary to meet all of its system development needs. Rather, it should focus R&D resources on military applications and rely on industry to the maximum extent possible to fund IT technology that can be adopted or adapted for defense use.

But doing business with the CIT industry has proven to be complicated. The industry is geared to a market of commercial business enterprise and consumers that dwarfs the defense market in both size and ease of doing business. Leading IT companies have limited incentives to do business with DOD, unless the department is willing to accept standard products without modification. And if DOD finds suitable technology, procurement is hampered by an acquisition system out of synch with commercial business practices. In the mid-1990s, DOD tried to increase procurement of CIT. Instruction 5000.2, the guide for DOD acquisition, was modified to state that defense systems will "make maximum use of commercial off the shelf technology." Numerous policy statements, speeches, and articles by high-level defense officials have emphasized this point.

Progress is being made, but more can be done. No one questions that DOD is doing a good job in applying CIT to enterprise and infrastructure requirements. Commercial products (telecommunications, computers, software, network servers, and routers) for virtually all DOD business enterprise requirements are procured rapidly and

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Horizons. Sweden's Use of Comercial Information Technology for Military Applications. October 2005, Number 50	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,Fort Lesley J.cNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**8**	

cost-effectively. On the military side—the information technology products that go into battlefield command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) systems or are imbedded in weapon platforms—the process slows down. Even tradeoff studies to determine the acceptability of commercial products to do the job are resisted. If CIT is not captured at a faster pace, DOD runs the risk of being unable to afford the capabilities required to complete missions and the further risk of losing the U.S. technological lead to any threat nation or group with the money to develop or buy the latest commercial products.

This issue was raised by Congress in fiscal year (FY) 2004 legislation that directed DOD to perform a study aimed at maintaining and improving the technological lead of the U.S. military by doing a better job of harnessing CIT in a timely, systematic fashion. Congress also asked whether the department could find ways to accelerate the acquisition of CIT.

DOD subsequently commissioned the Center for Technology and National Security Policy (CTNSP), an arm of the National Defense University (NDU) in Washington, DC, to undertake the study. Franklin D. Kramer, former Assistant Secretary of Defense for International Security Policy, was selected to chair the effort.

The objectives of the study were to examine the potential of CIT to meet military requirements, especially for products that must survive the harsh conditions of the battlefield; to determine the impediments to acquisition of acceptable CIT and search for ways to remove those impediments; and to examine the DOD acquisition process and recommend how it can be improved to provide a better climate for CIT.

The study, which was conducted from February to September 2004, featured wide participation by government acquisition and program management personnel, academics, and representatives of defense and commercial industries. A 2-day workshop at NDU brought these experts together to discuss the issues and make recommendations. The final report, which includes the findings, conclusions, and recommendations from the effort, has been briefed to senior leadership in the department. DOD has asked CTNSP to conduct a follow-on study in FY05, and that effort is under way.

Why Sweden?

In developing the methodology for the study, the team raised the question of how other allied or coalition nations addressed the utilization of CIT in military systems. Preliminary analysis had shown that although the United States is unquestionably the recognized global leader in IT, other industrialized nations were making rapid advances, as evidenced by such metrics as patents granted, per capita ownership of mobile phones, and use of e-commerce. It was generally agreed that the experience of other countries, especially the more technologically advanced countries of Europe that support standing military forces, could yield lessons applicable to improving the DOD process. The chairman approved a recommendation to examine other national programs, but limitations on time and resources restricted the analysis to a single country, Sweden.

A useful case study could have been drawn from several European countries. Certainly the United Kingdom, the closest of our allies, came to mind, as did Italy, France, and Germany. Despite drastically reduced defense budgets, each of these North Atlantic Treaty Organization (NATO) allies has invested in modern information technology to upgrade the command, control, communications, and intelligence of their national forces. However, it was the sense of the study team that these countries had been slow to adopt the concept of net-centric warfare and initiate development to achieve the requisite capabilities, and that their defense acquisition establishments had not been strong proponents of military use of commercial information technology.

Swedish acquisition policy requires that commercial technology be used in military systems wherever possible

In the next tier of smaller countries, Sweden stands out for its commitment to NCW, which Swedes call *network-based defense* (NBD). Sweden has had a major development program since 2001 to put network architecture in place, and Swedish acquisition policy requires that commercial technology be used in military systems wherever possible.

For a small nation, Sweden has a remarkable number of highly sophisticated and innovative CIT companies. According to the 2003 study *Facts about Information and Communications Technology in Sweden* by the Swedish Institute for Transport and Communications Analysis, at the end of 2000, 16,600 Swedish companies were designated as IT companies. They ranged in size from globally recognized giants such as Ericsson and Saab to startups with 1 to 5 employees. In general, they have proven to be leaders in technical innovation, are highly competitive internationally, and have benefited from government policies and support that have allowed them to flourish. In March 2000, the Parliament passed legislation establishing the objective that Sweden be the first country to become "an information society for all." The bill included an action plan for reaching that goal, including emphasis on IT education in the Swedish university system and broad investments to build a solid, sustainable foundation for continued growth of the Swedish IT industry. In 2003, the World Times Information Society Index designated Sweden the world's leading information economy for the fourth straight year. The ranking was based on a comprehensive index of statistics including personal computer and Internet usage, e-commerce, telecommunications infrastructure, broadband and wireless subscribers, and education levels.

Franklin D. Kramer (kramerf@ndu.edu) is a Distinguished Research Professor at the Center for Technology and National Security Policy. John C. Cittadino (JohnCit@aol.com) is President, JCC Technology Associates, Inc.

Swedish Armed Forces

With fewer than 9 million people, Sweden has had to rely on a combination of mandatory service and advanced technology to maintain a capable military force. In peacetime, the Armed Forces have approximately 20,000 personnel on duty, augmented by about 16,000 "conscripts" in training. This standing force is backed up by a home guard of approximately 100,000 men and women who could be mobilized if needed.

A 1999 review of defense policy and the military concluded that the Swedish homeland was not, for the foreseeable future, under danger of invasion, but nevertheless faced the same grave threats as other highly industrialized, affluent nations. The Parliament revised the direction of defense policy and announced that the Armed Forces should organize and equip to meet four strategic objectives:

- defend Sweden against armed attack
- uphold territorial integrity
- contribute to international peace and security
- strengthen society in the event of severe peacetime strains and emergencies.

The 1999 Parliamentary decision put the Swedish Armed Forces on a path of modernization to counter lack of manpower with sophisticated technology, mobility, and adaptability to meet new and unforeseen threats. Such a strategy is not unlike the U.S. approach to military transformation. At a national conference in Sälen, on January 21, 2004, the newly appointed Supreme Commander of the Armed Forces, General Håkan Syrén, stated that the threat picture

> has changed totally during the last decade. Old threats have dissolved and have been followed by very real threats emanating from large-scale terrorism and proliferation of weapons of mass destruction. These are threats that definitely cannot be neglected. To me, it is absolutely clear that from now on we need to be able to use military power to meet these types of threats and actions. *The primary focus of the Swedish Armed Forces in the near term should be to adapt and increase its capability to contribute to international crisis management tasks*.
>
> Our aim should be to create capabilities that are suited both for international tasks and national territorial defense tasks. We must not build separate capabilities for national and international tasks. Along with the immediate tasks, we have to maintain a long-term direction aiming at a capacity to understand and adapt to the military requirements of tomorrow. The network-based approach is an important part of this. We therefore also have to create units and prototype systems that are not necessarily needed or demanded in the short run. Their role is, instead, to increase our preparedness to manage unpredictable developments.

The Swedish defense system is in the process of radical renewal and modernization. The fundamental reason for this is the prevailing security situation, both internationally and in the vicinity of Sweden. Technological developments and the increased focus on international crisis management also are important factors in Swedish restructuring and reorientation.

Network-Based Defense

The network-based approach promoted by General Syrén has become a foundation for the restructuring of the Armed Forces. The Swedish Parliament, in 2001, passed a bill (2001/02:10 "Continued Renewal of the Total Defense") establishing that the "Armed Forces are to be developed according to the concept of network-based defense" and calling for a major development program to provide the network capability to implement the concept. Manuel W. Wik, Chief Engineer/Strategic Specialist of the Defense Materiel Administration (*Försvarets Materielverk* [FMV]), stated in a report entitled *Network Based Defense for Sweden: Latest Fashion or a Strategic Step into the Future?* that network-based defense (NBD) "has initiated the greatest change of the Swedish national defense in modern times. It is considered that the development in communications and information technology has opened up possibilities for a radical change of how military forces can be shaped and act."

NBD, like U.S. network-centric warfare, combines the application of communications and information technology to manage the acquisition and distribution of information across a military network to achieve the information superiority necessary to support a more flexible, dominant force. The military network is similar to the commercial Internet, with the addition of such requisite military features as priority, security, and restricted access. The analogy with the Internet becomes especially noteworthy when one recognizes that both the U.S. and Swedish programs are being developed largely using internationally accepted commercial standards and protocols contained in the DOD Joint Technical Architecture (JTA). The JTA is mandatory for all aspects of the Global Information Grid (GIG), which provides the network infrastructure to support U.S. network-centric operations. The Swedish NBD program is developing the equivalent of the GIG for the Swedish Armed Forces and has chosen to use the U.S. JTA as the starting point to define standards and protocols. Hence, the two networks probably will have a high degree of compatibility when access is authorized.

both the U.S. and Swedish programs are being developed using internationally accepted commercial standards contained in the DOD Joint Technical Architecture

Developing an infrastructure to support military networks of the magnitude of the GIG or NBD is a major undertaking that demands an evolutionary system-of-systems approach. Recognizing that development of the NBD requires a high level of experimentation and simulation, Sweden has established a national battlelab, also known as the Armed Forces C4ISR Development and Experiment Center, at Enkoping. The battlelab is essentially an integration and concept development test bed. The heart of the center is its simulation capability, which is capable of technical simulations and of generating a wide variety of military/homeland security scenarios. It includes cells for army, navy, air force, and civil personnel, who participate in scenario-based missions to demonstrate the capabilities of the evolving network to assess and refine network services.

The facility can remotely integrate military and civil command centers as well as military platforms such as tanks, ships, and planes to provide a wide capability for live and constructive simulation. It also acts as the hub for a network that ties more than a dozen locations throughout Sweden into the battlelab for remote participation in the experiments and demonstrations. The remote locations include industry sites, military bases, and government and university research centers. The remote nodes can use the battlelab to resolve integration issues as soon as they develop services and products for the NBD. The facility also allows widespread participation in the annual NBD demonstrations, which are the major function of the center.

The annual demonstrations are designed to measure progress and identify problems as the focus of the NBD "build a little, test a little" development philosophy. To date, there have been three of these demos. Complexity has increased from 6 participating military systems utilizing the 9 types of network services developed in 2002 to 16 systems utilizing some 33 types of service that had been developed by the 2004 demo.

In addition to its value as a technical support tool in the development process, the battlelab provides important inputs to refining service doctrine, concept of operation, tactics, techniques, and procedures, as well as the basis for new training curricula.

Swedish Government Views

The acquisition process for Sweden is centralized within the FMV. In this respect, it differs substantially from the American system, which delegates acquisition authority to the individual services and defense agencies, such as the Defense Logistics Agency. Given the smaller size of the Swedish military and the strongly joint approach of the Armed Forces Headquarters Staff, FMV is able to function as the "cradle to grave" manager of defense material. In this role, FMV has the responsibility to identify, define, and develop cost-effective solutions to meet military requirements. (In R&D, FMV works in close cooperation with the Swedish Defense Research Agency, the counterpart to the U.S. Defense Advanced Research Projects Agency.) FMV translates military requirements into system specifications for the development and procurement of individual systems. It also performs the role of systems architect by developing overall systems views and defining the role of individual material systems within the architecture as well as the requirements for integration. In carrying out this role, the FMV staff requires technical expertise, including an in-depth knowledge of the capabilities of the Swedish defense industry, as well as commercial capabilities (especially in IT) on an international scope.

The Swedish policy with respect to the application of CIT products and services to meet military requirements is virtually identical to DOD policy. As Birgitta Böhlin, Director General of FMV, stated in the 2002 FMV Annual Report:

> The restructuring of the Armed Forces is founded on what is known as Net Centric Warfare (NCW). NCW is concerned with information superiority, where systems have to be compatible with other systems so that relevant information can be gathered and sent quickly. NCW affects most materiel projects in progress due to new demands being made on operational and future systems. The result of the major Command and Control System Technology project provides an important foundation for the development of NCW. We also see a need for changed procurement strategies, where civil technology will be used to an ever-greater extent, resulting in new suppliers and increased international co-operation.

A 2003 FMV directive stated that commercial-off-the-shelf (COTS) technology shall be used whenever it meets the military requirements and compromises neither safety of personnel nor the protection of classified information.

affordable costs and rapidly advancing technology in the civil or commercial domain mandate the use of CIT wherever practical

Lieutenant Colonel Mikael Lindbergh, the Deputy Program Manager for the NBD Program, confirmed that it was necessary to examine CIT because the information services are the core of his program. He pointed out that a key to integration of CIT into NBD is the utilization of commercially based standards. He cited the use of the JTA, which is based primarily on internationally accepted commercial standards, as the basis for the program standards. He also referred to General Syrén's stated objective of a larger role for Sweden in international missions and the accompanying need to achieve coalition interoperability. He believes that as more nations adopt the JTA approach, the problems inherent in coalition interoperability will diminish.

Interviews conducted with representatives of the Armed Forces Staff, FMV, and the Swedish Embassy in Washington confirmed wide acceptance within the Swedish defense establishment that affordable costs and rapidly advancing technology in the civil or commercial domain mandate the use of CIT wherever practical.

The users, as represented by the Armed Forces Headquarters Staff, appear to fully support and encourage the use of CIT. A unit within the headquarters, the Joint Command, Control, Communica-

tions, Computers, and Intelligence Directorate, under Lieutenant Colonel Sten-Ake Larsson, has been established to monitor all Swedish development programs to determine their potential to utilize CIT. In programs where CIT is not evident and headquarters staff believes that there is potential for that particular project, the FMV and/or the responsible contractor is asked to show where CIT failed to meet requirements and set up a review process to reconsider the design approach.

Furthermore, where the establishment finds—for instance, in the case of a commercial software program—that the application does not conform to the established military way of carrying out missions and tasks, Larssen's office has the option of initiating a study to determine if the way of doing business should be brought into line with a more modern and efficient way of doing the job that is inherent in the methodology of the commercial software.

there are more similarities than differences between the American and Swedish processes to evaluate and acquire CIT for the military

Implementation of the policy to use CIT starts with the release to industry by FMV of a request for proposal (RFP). Wherever appropriate, the RFP is based on commercial specifications instead of military specifications. Vendors are encouraged to propose commercial solutions.

In the Swedish acquisition process, the norm is to conduct tradeoff analyses at the outset of system development to determine the risk/reward ratio of utilizing commercial technology versus initiating new development. Any evaluation includes a determination of whether the CIT can be used as is, or whether it requires modification or adaptation to do the job. Areas that are examined are the degree to which the CIT meets each facet of the requirement, including performance, security, safety, and the so-called "-ilities" (reliability, maintainability, sustainability, and so forth). When the CIT meets a subsystem requirement within a larger system, the issues of integration and testing of the technology are examined. These tradeoff studies include a life-cycle cost analysis of the specific CIT to form a basis to determine the cost-effectiveness of the approach versus a dedicated military development.

The Swedish process recognizes the potential shortcomings of CIT products in areas of reliability, maintainability, and sustainability. The tradeoff studies address these issues and search out solutions or workarounds. When the reliability of a CIT product fails to meet the military objective, answers are sometimes found in adapting the product to the military environment by embedding it in a protective package or case. As stated by one FMV engineer, "When the reliability is not up to standard, it is sometimes possible to buy two and still save money."

The Swedes are also coming to grips with the need to rethink how they maintain their systems as more and more commercial technology is accepted. Direct support from commercial contractors is increasing. Training in the use and maintenance of CIT is also under study. However, those interviewed are of the opinion that military personnel are becoming more technology-literate and more adept at grasping the inherent, intuitive training provided by companies for the civil marketplace.

Sustainability refers to maintaining a capability in service for the required time frame, which, in the case of the military, could be decades. Two facts associated with CIT are that commercial companies are introducing new product lines every 12–18 months, and the industry is volatile, with a relatively high number of failed companies each year. The Swedes state that this simply has not yet become a major problem for them. They are relying on a basic premise that the commercial industry will retain a high level of backward compatibility to satisfy its commercial customer base so that, as new products become available, for the most part, they will be plug-and-play into the NBD system. They recognize that they must remain aware of the commercial market, including the stability of the companies they plan to buy from. The FMV continually reviews CIT products and companies and publishes descriptions on its Internet site so that the information is available to everyone in the process.

The consensus Swedish assessment of the success or failure of the policy to use CIT is that it is too early to tell. This is easy to understand, given the newness of the policy and the early stages of the NBD program. Several examples of success were noted, such as the use of commercial hardware and software (the Windows operating system) for command and control (C^2) by the Swedish Implementation Force deployed to Bosnia, the use of ruggedized commercial computers and commercial software for logistics and message-handling on deployments to East Timor and Liberia, and the deployment of an Ericsson mobile cellular system with a commercial satellite communications reach-back to Kabul, Afghanistan, to support United Nations operations.

Discussions with Swedish officials indicated that there are more similarities than differences between the American and Swedish processes to evaluate and acquire CIT for the military. Probably the most noteworthy difference is that the Swedish system of tradeoff analysis appears to be routinely applied in Sweden, where the policy to use CIT is widely accepted at the working level, whereas the United States has a much less consistent approach, with less than enthusiastic acceptance of the policy by both government and defense contractor personnel.

Swedish Industry Views

Interviews were conducted with a representative group of Swedish industry, including major defense integrators Saab (both the military aircraft and command, control, communications, and intelligence divisions) and Ericsson, and smaller companies, such as Sectra (a supplier of cryptographic systems), SweDish (a supplier of commercial satellite communications terminals), and Effnet (a small commercial company specializing in network software). All of the companies voiced solid support for the government policy to use CIT

whenever practical. Where they differed was in a view expressed by small companies that the "big companies support the policy publicly, but they are all too often trying to make more money by developing things on their own." (It should be noted that similar concerns were voiced by one or two government officials about the willingness of the larger integrators to avoid costly developments through the acceptance of COTS technology.)

Saab (Command, Control, and Communications Division) and Ericsson, which, along with Boeing and IBM of Sweden, make up the team developing the NBD system of systems, tended to discuss CIT in terms of NBD. Goran Kristoffersson of Saab reemphasized the vital role played by international commercial standards and protocols. Both companies complimented the government's encouragement to use CIT and cited FMV willingness to examine CIT tradeoff studies. Saab representatives estimated that their company's recent experience in developing C^2 systems showed that approximately 50 percent of the software used was commercial. Ericsson executives commented that, in their work on NBD software, all of the operating systems are commercial and 75 percent of the middleware is commercial. In the area of communications products and services, Ericsson stated that the military uses 100 percent commercial technology everywhere except for tactical operations. There has been no decision to accept other than military specification radios and communication devices at the tactical level, but Ericsson stated, without providing details, that there have been signs that this position may change in the near future.

Robin von Post of Sectra echoed this view and commented that he saw more of a willingness to take on the risk of CIT in Sweden than in the United States. He went on to say that "RFPs out of FMV invariably include statements encouraging commercial solutions," and that FMV is a very flexible buyer that is always willing to listen to challenges to requirements in the hope of finding a more cost-effective solution.

Johan Kihl, former Vice Chief Staff of the Armed Forces and currently a consultant to Ericsson, stated that "in today's world, where the threat of high-intensity warfare is no longer imminent, but a myriad of low-level threats are just waiting to happen, we can no longer afford, nor do we need, the pure military solution. We must look to commercially based solutions as the norm, not the exception." He mentioned that, to stay abreast of commercial developments, Sweden has initiated a structure of committees with representatives from the Armed Forces, the Swedish R&D establishment, and industry that meets 3 or 4 times a year.

Anders Lange, General Manager for Business Development at Ericsson, mentioned that the FMV is learning to act as a buyer in the commercial world and that perhaps DOD has to learn to do the same. When asked to expand, he offered the following:

> I am referring to business practices in the commercial telecoms industry. Operators (the buyers) and vendors (the suppliers) alike all take active part in standardization of functions and interfaces. Once standards have been settled, vendors compete for contracts. Since telecommunications are global, operator-specific solutions are practically nonexistent. The way operators influence the vendors (and exercise some amount of control) is through standardization, price pressure, and release date constraints. What I am aiming at for DOD is to take part in this (commercial process) on equal terms with the telecoms industry, i.e., participate in standardization work, actively drive standardization areas such as security (for the benefit of society at large), and then perform purchases much in the way operators do (frame agreement contracts, long-term relations with one or two vendors). Where military modifications/reinforcements are needed, these should be implemented without altering any of the agreed international standards.

the policy to optimize the utilization of CIT has been extended to state-of-the-art weapons systems

The policy to optimize the utilization of CIT has been extended to state-of-the-art weapons systems in a big way. Given the fact that high-performance weapons systems require very high subsystem reliability, one might expect a reluctance to employ CIT in these applications. This expectation was quickly dispelled in a meeting with Anders Pettersson, Program Director of Research and Technology for Saab Aerosystems' new Gripen Mark 3, a high-performance fighter aircraft. Pettersson walked through a block diagram of Gripen subsystems, pointing out those that employed CIT. Some examples were: a fair amount of software, including Windows NT as the operating system for the mission control computer, commercial processors (INTEL and Power PC) and central processing unit boards in the flight system and mission control systems, replacement of the military specification data bus with a local area network using a commercial Internet protocol, and commercial laptop computer display technology in the cockpit.

Ericsson Microwave, the manufacturer of state-of-the-art radar systems for the Gripen as well as other tactical air, maritime, and ground applications, reported the same wide use of CIT products in these systems. Again, it was made clear that industry takes very seriously the mandate to use CIT wherever practical.

Pettersson also pointed out that commercial companies normally do business with the government through the prime contractors (usually Saab or Ericsson) on purely commercial terms. It then becomes the responsibility of the primes to do the necessary integration and testing to receive government certification that the system/equipment is acceptable for operational use.

The Swedish application of CIT in modern, high-performance weapons systems has parallels in the United States. For example, the F–35 Joint Strike Fighter (JSF) program, proclaimed as the largest DOD acquisition program since the Manhattan Project, utilizes considerable CIT in its development. The Integrated Core Processor (ICP), the central computer system for the JSF, is being implemented in an open-system architecture designed to maximize the use of commercially available products and standards. The ICP supports all of the embedded computing elements for multiple

aircraft subsystems, including the digital signal processing for the sensors and cockpit displays.

According to Bob Coultas, hardware program manager for the ICP for JSF prime contractor Lockheed Martin, "Incorporating COTS technology into an open-system architecture throughout the F–35 will enable frequent technology updates at low cost . . . open-system architecture is based on the use of commercial, standard interfaces that enable the program to take advantage of commercial technologies for more supportable, lower-cost designs. Affordability is the cornerstone of the F–35 program, and has been designed into the F–35 aircraft from day one."

Emergency Management

The Swedish Emergency Management Agency (SEMA) is the equivalent of the U.S. Department of Homeland Security (DHS), and its relationship with the Swedish Armed Forces is similar to the DHS relationship with the U.S. military; each has its discrete areas of responsibility but is prepared to work closely with the Armed Forces under certain circumstances, such as an external terrorist attack.

In late 2002, SEMA initiated development of a national emergency radio communication network called RAKEL at an estimated cost of 2.3 billion Swedish kroner (approximately U.S. $700 million). Under the overall management of SEMA, the network will be used by local fire, police, and ambulance services, and the Coast Guard, Customs Department, and Armed Forces. (When queried about the relationship between RAKEL and the communications envisioned for the NBD system, SEMA officials indicated that it was too early to predict what role the radio network might play.) In March 2003, FMV, which also serves as the acquisition agency for SEMA, issued an RFP that did not define a technical solution or include a technical specification. Rather, it contained a nontechnical description of user needs. Proposals were received for a number of technical approaches, including commercial cellular systems from Ericsson and Nortel.

In March 2004, following evaluation of numerous proposals, FMV awarded a contract to a consortium of Saab, Nokia, and Eltel Networks (formerly Swedia Networks) to build the RAKEL network, which will provide coverage to 85 percent of the country and 99 percent of the population. The Saab approach, which will require between 2,000 and 2,500 base stations, is based on the European commercial radio standard known as terrestrial trunked radio (TETRA).

A factor in the choice of a TETRA-based solution was interoperability with first responders in neighboring countries. TETRA has its roots in a 1996 NATO decision to release a number of frequencies in the ultra-high frequency (UHF) band for the purpose of establishing a trans-Europe frequency band for public safety emergencies. These released frequencies are found in three slots in the UHF band (380–400, 410–430, and 450–470). The European Telecommunication Standards Institute picked up on the NATO decision and developed the TETRA standard, based on time division, multiple access specifically to support emergency and public service needs. TETRA offers services for direct mode (direct calls between terminals), standard switched calls, group calls, priority control, and fast-through connect. TETRA handheld and vehicular sets are capable of 4-channel operation, with each channel transmitting up to 7.2 kilobits of data. The vehicular sets also can act as automatic relays to maintain network connectivity. The air interface is encrypted, using the TETRA Encryption Algorithm 2. Public safety organizations throughout Europe quickly saw the advantages of TETRA, and Nokia, Marconi-Selenia, Motorola, and other manufacturers developed communications products to meet the demand.

When relating the Swedish approach to RAKEL to the situation in the United States, the overriding lesson to be learned is not in the TETRA technology being employed, nor in the use of primarily commercial technology, but in the fact that all organizations within Sweden (local, regional, and national) responsible for responding to an emergency or crisis will use common, interoperable communication equipment—and that sister organizations in neighboring countries will be using the same system. Contrast this with the United States, where communication systems are bought at the local level. Given little if any coordination even among departments in the same city, it is easy to understand how "lack of interoperable communications" is identified as a major deficiency by every study dealing with security readiness since September 11, 2001.

Because of the separation of national, state, and local governments in the United States, an amendment to the Constitution might be necessary to adopt the Swedish model and require a single system for all users nationwide. However, DHS could work with DOD on a set of open standards for a national communication system for all emergency organizations. Industry undoubtedly would respond to a national market by developing competitive, interoperable equipment, as happened in the case of TETRA in Europe. At the state and local level, legacy systems could be replaced as budgets permit with the assurance that neighboring organizations could join a network of interoperable systems as they are upgraded.

Conclusions and Recommendations

The Swedish approach to military use of commercial information technology cannot simply be transplanted to the United States. For one thing, Swedish policies in this area are new, and Sweden is still learning how to acquire CIT and how to do business with companies on commercial terms. The government believes it has evolved a process to sort out the limitations of CIT, make the necessary adaptations, and integrate CIT into military warfighting systems, but does not yet have much experience with the results. Also, Sweden enjoys many advantages over the United States in procurement innovation: the nation and its military forces are small, and fewer and smaller programs simplify monitoring for CIT applicability and performing tradeoff studies to ascertain acceptability. Also, acquisition is centralized, and a small (20-person) headquarters staff can ensure that the policy of employing CIT is being followed to the highest degree practical. Moreover, many of Sweden's military systems are procured internationally. Nevertheless, several recommendations can be derived from Swedish successes to date.

Establish a center of excellence to monitor the status of CIT and publish information online for all DOD developers. The Swedish FMV has found that capitalizing on the benefits of CIT requires

staying current with commercial products and the emerging standards that precede new products. With the help of Swedish industry, the FMV maintains surveillance and publishes online CIT information useful to industry and government engineers and managers. A similar service could be performed by a U.S. Center of Excellence for CIT. Such a center could be established at U.S. Joint Forces Command in conjunction with its C4ISR test-bed capability.

Establish a methodology to be used by all DOD acquisition centers to review new developments and major upgrades for applicability of CIT to meet requirements. The vast size of the U.S. system, with thousands of individual programs, requires visibility at the service and agency acquisition centers to assure that CIT utilization is optimized. This would present an opportunity for DOD to develop a standard methodology that would require the development of a CIT tradeoff analysis to be used throughout the department. Such a methodology could be developed at the Defense Acquisition University.

Include in the Defense Acquisition Board (DAB) process a requirement to present tradeoff analysis on CIT considered to meet program requirements. One of the major hurdles within the DOD acquisition process has always been the necessity to introduce a certain degree of discipline to insure that department policies are carried out uniformly (unlike Sweden, where the acquisition community, both government and industry, appears to be implementing CIT policy uniformly). Within DOD, the DAB process has established a checklist methodology for those development/acquisition programs that meet certain criteria for size, dollar value, priority interest, and so forth. It would appear (given the development of the methodology discussed above) that the DAB checklist should include tradeoff analysis of the utilization of CIT in major programs.

Rather than develop a new system (primarily software) to meet the way the organization has always done business, encourage the user to consider changing the way of doing business when a CIT product implements a more efficient/effective way. Historically, one of the failures of DOD's efforts to automate at all levels, from tactical computers on the battlefield to business enterprise systems that manage finance and personnel, results from the demand that contractors automate manual methods of doing business. Only after decades of inefficient operation was it realized that re-engineering of processes is required to allow automated systems to optimize productivity. The business community has recognized this for many years, and it is reflected in the commercial software on the market to improve business functions of every type. The Swedish Armed Forces have also accepted that the real benefits of commercial software for many applications lie not in the lower initial cost of the software but in the increased productivity that results from adapting the military process to capture improved functionality; now they change traditional methods of operation to capture the increased productivity offered by commercial software. DOD would do well to issue a policy directive encouraging this approach. Indeed, there are indications that DOD is moving in this direction. A recently released Army RFP on the General Financial Enterprise Business System states that the system will use commercial software and that the users are prepared to change their traditional processes to accommodate the model of the chosen software.

Introduce more flexibility in acquisition by providing a statement in all RFPs that use of CIT is encouraged and that tradeoffs, including the opportunity to challenge specifications, are invited. This is the practice in Sweden, and it has been employed sporadically in DOD requests for proposals. Such a statement in RFPs would at least give the acquisition authority a better understanding of what the government is paying for certain specification requirements.

Explore methods of motivating defense contractors, especially the major system integrators, to use more CIT versus tailored development. There was little evidence that the FMV provides any extraordinary motivation to Swedish prime contractors to optimize the use of CIT. This is attributed to the perception that the working relationship between Swedish industry and the government is one of close cooperation and that industry has fully endorsed the FMV policy on CIT. In the United States, the motivation of defense primes appears to be dominated by the bottom line; if a company can increase profit by avoiding CIT in favor of tailored development, it usually follows the dollars. An examination of the pros and cons of applying various motivational tools available to U.S. contracting officers certainly appears to be in order.

the real benefits of commercial software lie in the increased productivity that results from adapting the military process

Take a more proactive role in international standards organizations to influence and stay abreast of commercial standards that drive new technology. The suggestion to play a more proactive role on standards bodies came from Swedish industry. The view was expressed several times that the key to seamless utilization of CIT is to promote an open architecture based on commercial standards. This is certainly the approach of the U.S. GIG and the Swedish NBD. But the rate of technology turnover requires constant monitoring of the commercial standards process to avoid obsolescence. Furthermore, certain attributes required in a military network, such as information assurance and priority of service, do not necessarily have high priority in the commercial world. Without participation in these international bodies to argue for military features to be embedded in standards, down the line the military will face products that either do not meet their needs at all or require costly adaptation.

Defense Horizons *is published by the Center for Technology and National Security Policy. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.*

Center for Technology and National Security Policy

Hans Binnendijk
Director